The official voice of the Air Force Research Laboratory

news@afrl

CIO Topics

Winter 2001 Volume II, Issue 4

OPSEC: Illusion or fact…Minimizing the risk

by Teresa Anderson, HQ AFRL Security Office

WRIGHT-PATTERSON AFB, Ohio --- Is our trash someone else's treasure? Do we protect our sensitive information from unauthorized access? Are we looking at our OPSEC program from the eyes of our adversaries? These are simple questions that you need to ask yourself when dealing with sensitive unclassified information.

How could someone, seemingly just like you and me, steal our technology? A frequently asked questions that is actually very difficult to answer. Answering why they did it, convicted spies themselves have collectively identified a number of motivating factors for spying, often in combinations, they are: sense of anger, disaffection, revenge - getting back at "the system" or a specific person.

Anger is the most prevalent motivation found in espionage. Greed and financial need is another top reason they have the perception that money can fix anything, that it can buy happiness. The adventure or thrill of the act, which in their minds would add excitement to an otherwise boring life is an increasing reason of why they spy. Another could be ego or self-image, to try to repair wounds to self-esteem and this is often coupled with anger and revenge. A desire to please or win the approval of the foreign intelligence officer who has been recruiting that person is called ingratiation and is considered one of the top reasons for spying. The sense of helping the "underdog", perhaps because they feel like an "underdog" themselves is a spying reason referred to as identification/ideology attempts.

There is no absolute prevention. Certain measures can possible deter or at least detect espionage. You can play a real and vital role in this effort. Be especially alert to the situational stressors and personality characteristics that lead people to consider espionage as a way of solving problems.

Preventative Measures must be taken to guard against spies. Some of them include simple techniques such as the "trash can". Don't throw anything in the trash that you would not want to hand to a spy. Don't try to talk around sensitive topics over an unsecured telephone line. Ensure everyone you are dealing with has a need-to-know before you release any sensitive information to him or her. Use of shredders for destruction of program information is a necessity to preventing unauthorized disclosure of your critical information.

I can't stress it enough that you have to take OPSEC seriously in protecting your information. Always ask yourself, "Will this information that I am dealing with, if released into an adversaries hands cause damage to our national security"? If the answer is yes, then PROTECT IT and take the appropriate measures to not allow it to fall into the wrong hands.

Your Operations Security (OPSEC) program should be designed to prevent unauthorized disclosure of sensitive unclassified information falling into the hands of our adversaries. OPSEC provides a holistic picture of our operation, from the outside in. It is a systematic process that looks at our mission through the eyes of an adversary. Your OPSEC processes should identify your critical information, be able to analyze the threat to that information, discover the vulnerabilities and develop appropriate countermeasures based on the vulnerability and inherent risk.

An internal review of all technical material should be approved/coordinated by your OPSEC Security Program Manager within your organization prior to public release to ensure no critical information is present to include internet postings, success stories etc.

If you believe that someone may be contemplating espionage or other criminal activity, or has taken steps to initiate it, you are obligated to immediately report this information to your Security/Counterintelligence Office.

So again let me ask you these two questions, do you have a solid OPSEC process that protects your information and technology? How do you look at your OPSEC program as fact or fiction?

Espionage is alive and well especially here at Wright-Patt. Don't fool yourself into thinking that our adversaries do not want our information. Science and Technology for tomorrow's aerospace forces is our allegiance; to protect that technology should be our privilege and duty. You are the one who keeps our technology protected, our nation secure and our world a safer place.

So the next time you throw something away remember what we may see as trash could be our adversaries treasure. **@**